

SUMMARY OF POINTS OF GENERAL COMMUNICATION, INC.
with respect to Lifeline database development
WC Dockets No. 11-42 and 03-109, CC Docket No. 96-45
(June 13-14, 2011)

I. Database Administration

- Some fundamental points:
 - A database either for duplicate control or eligibility confirmation is a program administration function, not a compliance function. Thus, it is appropriate created and funded by or at the direction and supervision of the FCC and the Administrator (USAC).
 - The database cannot be operated by a group of carriers. Neutrality and confidentiality are of paramount importance so as not to skew competition among carriers to serve Lifeline-eligible individuals. The Commission in other settings has required neutrality (e.g. numbering administration, porting and pooling).
 - It is not appropriate to require a subset of carriers to fund these functions over the long term. As an expense of universal service administration, the costs should be supported by the Universal Service Fund, and thus become part of the contribution base. Query charges could disincent Lifeline marketing and subscription.
- Who contracts for the database providers?
 - With the costs borne out of the USF, it makes most sense for either the FCC or USAC to undertake contracting for the provision of the database.
 - Because ETCs will need to be able to interact with the database provider, it may make sense to have a technical advisory committee to help develop specifications and interfaces for the database.
- One or multiple database providers?
 - This is a question that the FCC ought to decide. This is not just a technical question but involves issues of procurement policy and the best structure for long term cost minimization and quality services.

- Extant FCC models:
 - Number Portability – There is a single, national database administrator today. As a separate model, the original implementation would have had two administrators serving different, non-overlapping regions of the country.
 - White Spaces – FCC has approved multiple database providers, all of whom can serve anywhere in the country and must synchronize their databases.

II. Data Security & Privacy

- “Garbage In, Garbage Out.”
 - Who and how many will be inputting to the database?
 - Need to have systems to validate data and maintain accuracy.
 - Likely need to have a way to permit individuals to verify and correct their own records. *See* 5 U.S.C. § 552a(d).
 - Need have a way to deal with situations in which there is no USPS standardized postal address, or the postal address is a communal post office box. In Alaska, there are a lot of villages that are not in the USPS database.
- Managing access and permitted uses.
 - If queries at the time of customer sign-up are anticipated, what marketing uses are precluded? Can a carrier simply crash addresses against the database to develop a list of potential Lifeline customers? If not, what prevents that?
 - Broad access increases the likelihood of a data breach.
- Privacy.
 - Employ “Privacy by Design” – “Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy.” Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* at v (December 2010).
 - By necessity, the information will be personally identifiable.

June 13-14, 2011

- The Commission cannot use the whole social security number without express statutory authorization. *See* Privacy Act § 7, 5 U.S.C § 552a note (“It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.”); *see also* *Ingerman v. Delaware River Port Authority*, 630 F. Supp. 2d 426, 442 (D. N.J. 2009)(invalidating requirement of social security number for an EZ Pass seniors discount, which was collected in part to prevent fraud).
- Compelling carriers to retain data for audits also presents a privacy risk. FCC should minimize record retention requirements for audit to protect privacy. *E.g.*, in federal default states, today carriers cannot be required to retain copies of documentation of income-based eligibility.